

Машина Энигма

Содержание

Введение	3
1. Принцип работы шифровальной машины Энигма, её достоинства и недостатки	5
2. Алгоритм работы Машины Энигмы и реализация графического интерфейса	8
3. Тестирование разработанной программы	12
Заключение.....	15
Список использованных источников.....	16

Введение

Эни́гма (от нем. *Änigma* — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Первую версию роторной шифровальной машины запатентовал в 1918 году Артур Шербиус. На основе конструкции первоначальной модели Энигмы было создано целое семейство электромеханических роторных машин под тем же названием, применявшихся с 1920-х годов в сфере коммерческой и военной связи во многих странах мира, но наибольшее распространение получили в гитлеровской Германии во время Второй мировой войны. Именно германская военная модель чаще всего подразумевается при упоминании Энигмы.

Впервые шифр Энигмы удалось дешифровать в польском Бюро шифров в декабре 1932 года. Четверо сотрудников разведки с помощью данных французской разведки, математической теории и методов обратной разработки смогли разработать и построить специальное устройство для дешифровки закодированных сообщений, которое называли «криптологической бомбой». После этого немецкие инженеры усложнили устройство Энигмы и в 1938 году выпустили обновлённую версию, для дешифровки которой требовалось построить более сложные механизмы.

9 мая 1941 года при захвате силами Великобритании подводной лодки U-110 в руки союзников впервые попала шифровальная машина Энигма вместе с кодами, радиограммами и другими связанными документами. С помощью полученных материалов английские криптографы начали чтение сообщений немецких подлодок, использовавших «Дельфин» на трёхроторной Энигме.

В августе 1941-го англичане создали более совершенные «Бомбы», позволившие им оперативно расшифровывать немецкие радиограммы. Через два месяца немцы ввели новый код для подлодок, но Блетчли-парк сумел взломать и его.

Англичане читали вражеские шифрограммы до февраля 1942-го, когда немецкий флот начал использовать новую четырёхроторную Энигму. Ситуацию удалось исправить только когда 30 октября 1942 года противолодочный корабль Petard захватил модернизированную Энигму и документацию к ней с подводной лодки U-559. Это позволило расшифровывать немецкие сообщения до самого конца войны.

Целью работы является программная реализация Машины Энигма с интерфейсом.

Для достижения указанных целей были поставлены следующие задачи:

- Изучение принципа работы Машины Энигма.
- Разработка программы Машины Энигма с интерфейсом.
- Тестирование разработанной программы.

1. Принцип работы шифровальной машины Энигма, её достоинства и недостатки

В Энигме имелось три отсека для помещения трех роторов и дополнительный отсек для размещения рефлектора. Всего за время Второй мировой войны было изготовлено восемь роторов и четыре рефлектора, но одновременно могло использоваться ровно столько, на сколько была рассчитана машина. Каждый ротор имел 26 сечений, что соответствовало отдельной букве алфавита, а также 26 контактов для взаимодействия с соседними роторами. Как только оператор нажимал на нужную букву, — замыкалась электрическая цепь, в результате чего появлялась шифрованная буква. Замыкание цепи происходило за счет рефлектора.

На рисунке 1.1 представлена иллюстрация нажатия клавиши «А» с последующей дешифрацией в букву «G». После ввода буквы крайний правый ротор перемещался вперед, меняя тем самым ключ.

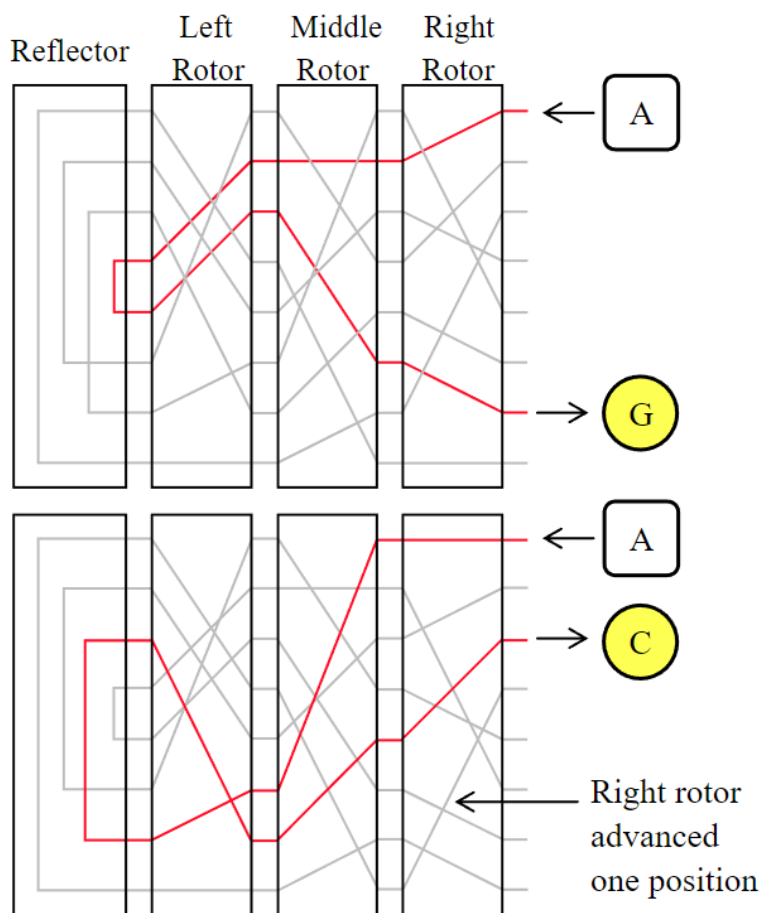


Рисунок 1.1 – Принцип работы шифровальной машины Энигма

Например, если на вход первого ротора поступала буква «N», то на выходе должна быть только «W» и никакая другая буква больше. При попадании этой буквы на второй ротор, она бы уже преобразовалась в «T» и т.д. То есть, каждый ротор выполнял четко поставленную задачу в плане коммуникации.

В таблице 1.1 представлено 8 различных роторов.

Таблица 1.1 – Роторы

Rotors\Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Turnover
Rotor 1	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	Q
Rotor 2	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	E
Rotor 3	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	V
Rotor 4	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B	J
Rotor 5	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K	Z
Rotor 6	J	P	G	V	O	U	M	F	Y	Q	B	E	N	H	Z	R	D	K	A	S	X	L	I	C	T	W	ZM
Rotor 7	N	Z	J	H	G	R	C	X	M	Y	S	W	B	O	U	F	A	I	V	L	P	E	K	Q	D	T	ZM
Rotor 8	F	K	Q	H	T	L	X	O	C	B	J	S	P	D	Z	R	A	M	E	W	N	I	U	Y	G	V	ZM

В таблице 1.2 представлено 4 различных рефлектора.

Таблица 1.2 – Рефлекторы

Reflector B	(AY)	(BR)	(CU)	(DH)	(EQ)	(FS)	(GL)	(IP)	(JX)	(KN)	(MO)	(TZ)	(VW)
Reflector C	(AF)	(BV)	(CP)	(DJ)	(EI)	(GO)	(HY)	(KR)	(LZ)	(MX)	(NW)	(TQ)	(SU)
Reflector B Dunn	(AE)	(BN)	(CK)	(DQ)	(FU)	(GY)	(HW)	(IJ)	(LO)	(MP)	(RX)	(SZ)	(TV)
Reflector C Dunn	(AR)	(BD)	(CO)	(EJ)	(FN)	(GT)	(HK)	(IV)	(LM)	(PW)	(QZ)	(SX)	(UY)

Пройдя через 3 ротора, символ подается на фиксированную отражающую пластину (рефлектор), которая представляет собой просто замену букв парами. Выход из него, в свою очередь, проходит через роторы в обратном направлении, возвращаясь на входной диск, представленный на рисунке 1.1.

Таким образом, Энигма выполняет последовательно семь замен: тремя колесами, затем заменой отражателя, затем тремя колесами в обратном направлении.

Большим недостатком шифровальной машины Энигма, можно сказать, стала ее сложность кодирования. При кодировке текста буква не шифровалась, как она есть. Например, буква «R» никогда не могла стать буквой «R». Зная это, противник получал часть информации, необходимой для расшифровки.

Вторым минусом являлось то, что Энигма шифровала первые три буквы повторно. Это позволяло найти шаблоны шифра.

Также недостатком являлась сама неосторожность немцев. Составляя текст сообщений, они начинали его словами о погоде и заканчивали традиционным приветствием. В итоге дешифровальщик, опираясь на эти знания и отгадав пару слов, мог подобрать ключ кодировки.

Но, даже с учётом всех недостатков машины Энигма, расшифровать код немецкой шифровальной машины было практически невозможно. Не хватало ни времени, ни людей. Зашифрованные послания, переданные через Энигму, каждый день имели новый ключ и множество вариантов расшифровки. Со времен Второй мировой войны остались зашифрованные с помощью Энигмы сообщения, которые до сих пор не раскодировали. Они есть в открытом доступе на некоторых сайтах. Найти ключ к ним пытаются уже более 70 лет.

2. Алгоритм работы Машины Энигмы и реализация графического интерфейса

Под сдвигом вправо понимается движение ротора по часовой стрелки, под сдвигом влево понимается движение ротора против часовой стрелки.

$shift$ – позиция буква в исходном слове, $shift_{R1}$ – сдвиг ротора 1, $shift_{R2}$ – сдвиг ротора 2, $shift_{R3}$ – сдвиг ротора 3.

- 1) Нахождение парного символа для кодируемого символа на коммутационной панели, если такой имеется.
- 2) Сдвиг символа вправо на $shift_{sum1} = shift + shift_{R1}$.
- 3) Преобразование символа ротором 1.
- 4) Сдвиг символа влево на $shift_{sum2} = shift_{sum1} - shift_{R2}$.
- 5) Преобразование символа ротором 2.
- 6) Сдвиг символа вправо на $shift_{sum3} = shift_{sum2} - shift_{R3}$.
- 7) Преобразование символа ротором 3.
- 8) Сдвиг символа влево на $shift_{R3}$.
- 9) Преобразование символа рефлектором.

Обратная процедура:

- 10) Сдвиг символа вправо на $shift_{R3}$.
- 11) Обратное преобразование символа ротором 3.
- 12) Сдвиг символа влево на $shift_{sum3}$.
- 13) Обратное преобразование символа ротором 2.
- 14) Сдвиг символа вправо на $shift_{sum2}$.
- 15) Обратное преобразование символа ротором 1.
- 16) Сдвиг символа вправо на $shift_{sum1}$.
- 17) Нахождение парного символа на коммутационной панели, если такой имеется.

Исходные данные для шифрования:

- Исходное слово для шифрования – «IT».
- Коммутационная панель – «C-I, R-U».
- Ротор 1 – «Тип 3», смещение – «0».
- Ротор 2 – «Тип 2», смещение – «0».
- Ротор 3 – «Тип 4», смещение – «0».
- Рефлектор – «Тип C».

Пример шифрования слова «IT» представлен на рисунке 2.1.

Input: IT

Patch Panel: C-I, R-U

Rotor 1: 3 Shift: 0 Rotor 2: 2 Shift: 0 Rotor 3: 4 Shift: 0 Reflector: C

Output: RE

T → T → V → M → K → L → L → I → I → E → E → A → A → A → C → G → E → E

Elements	Values																										Turnover	Shift
Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Patch panel	A	B	I	D	E	F	G	H	C	J	K	L	M	N	O	P	Q	U	S	T	R	V	W	X	Y	Z		
Rotor 1	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	V	0
Rotor 2	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	E	0
Rotor 3	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B	J	0
Reflector	F	V	P	J	I	A	O	Y	E	D	R	Z	X	W	G	C	T	K	U	Q	S	B	N	M	H	L		

Рисунок 2.1 – Пример шифрования

Пример дешифрования слова «IT» представлен на рисунке 2.2.

Input:

Patch Panel:

Rotor 1: Shift: Rotor 2: Shift: Rotor 3: Shift: Reflector:

Output: IT

→ → → → → → → → → → → → → → → → →

Elements	Values	Turnover	Shift
Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z		
Patch panel	A B I D E F G H C J K L M N O P Q U S T R V W X Y Z		
Rotor 1	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O	V	0
Rotor 2	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E	E	0
Rotor 3	E S O V P Z J A Y Q U I R H X L N F T G K D C M W B	J	0
Reflector	F V P J I A O Y E D R Z X W G C T K U Q S B N M H L		

Рисунок 2.2 – Пример дешифрования

В поле «Input» вводится слово, необходимое для шифрования/расшифрования.

В «Patch Panel» (коммутационная панель) вводятся пары букв через тире, которые заменяются друг другом.

В поля «Rotor» (ротор) 1-3 указывается тип ротора и его смещение.

В поле «Reflector» (рефлектор) указывается тип рефлектора.

Изменения коммутационной панели, роторов и рефлектора отображаются в таблице, представленной на рисунке 2.3.

Elements	Values																										Turnover	Shift
Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Patch panel	A	B	I	D	E	F	G	H	C	J	K	L	M	N	O	P	Q	U	S	T	R	V	W	X	Y	Z		
Rotor 1	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	V	0
Rotor 2	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E	E	0
Rotor 3	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B	J	0
Reflector	F	V	P	J	I	A	O	Y	E	D	R	Z	X	W	G	C	T	K	U	Q	S	B	N	M	H	L		

Рисунок 2.3 – Таблица значений элементов Машины Энигмы

На основе введенных данных шифруется/дешифруется заданное слово. Результат шифрования слова «IT» представлен на рисунке 2.4.

Output: RE

Рисунок 2.4 – Зашифрованное слово для исходного слова «IT»

Под полем «Output» выводится путь шифрования/дешифрования буквы, представленный на рисунке 2.5. (Начальная буква – введенная последняя буква, конечная буква – зашифрованное/расшифрованная буква).

T → T → V → M → K → L → L → I → I → E → E → A → A → A → C → G → E → E

Рисунок 2.5 – Путь шифрования буквы T

Подробный результат шифрование/дешифрования последней введенной буквы представлен на рисунке 2.6.

Красным цветом показан путь прохода шифрования/дешифрования буквы до рефлектора, синим – обратный путь.

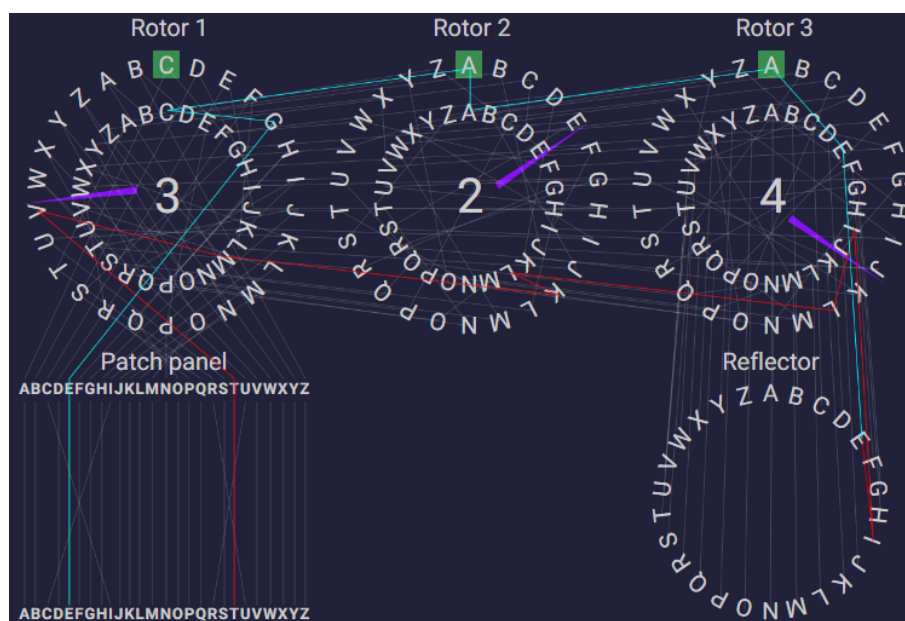


Рисунок 2.6 – Подробный путь шифрования буквы T

3. Тестирование разработанной программы

Пусть входная последовательность для шифрования будет FG.

На рисунке 3.1 представлено шифрование символа F.

Input:

Patch Panel:

Rotor 1: Shift: 3 Rotor 2: Shift: 0 Rotor 3: Shift: 2 Reflector:

Output: Z

→ → → → → → → → → → → → → → → → →

Elements	Values	Turnover	Shift
Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z		
Patch panel	A B I D E F G H C J K L M N O P Q U S T R V W X Y Z		
Rotor 1	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J	Q	3
Rotor 2	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E	E	0
Rotor 3	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O	V	2
Reflector	Y R U H Q S L D P X N G O K M I E B F Z C W V J A T		

Рисунок 3.1 – Шифрование символа F

На рисунке 3.2 представлено шифрование последовательности FG.

Input:

Patch Panel:

Rotor 1: Shift: 3 Rotor 2: Shift: 0 Rotor 3: Shift: 2 Reflector:

Output: ZW

→ → → → → → → → → → → → → → → → →

Elements	Values	Turnover	Shift
Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z		
Patch panel	A B I D E F G H C J K L M N O P Q U S T R V W X Y Z		
Rotor 1	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J	Q	3
Rotor 2	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E	E	0
Rotor 3	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O	V	2
Reflector	Y R U H Q S L D P X N G O K M I E B F Z C W V J A T		

Рисунок 3.2 – Шифрование последовательности FG

Алгоритм кодирования последовательности FG:

- 0) На вход поступает символ F. shift = 1.
- 1) Проверяется, нет ли у символа F парного символа в коммутационной панели. Если нет, то символ без изменений передается дальше. В

противном случае он заменяется на тот, который находится с ним в паре. В нашем случае символ F не претерпевает изменений.

- 2) Далее происходит сдвиг на 4 вправо ($\text{shift}_{sum1} = \text{shift} + \text{shift}_{R1} = 1 + 3 = 4$) по алфавиту. Таким образом получаем символ J.
- 3) Ротор 1 преобразует J в Z (таблица 1.1).
- 4) Далее происходит сдвиг 2-го ротора влево на 4 по алфавиту ($\text{shift}_{sum2} = \text{shift}_{sum1} - \text{shift}_{R2} = 4 - 0 = 4$). $Z \rightarrow V$.
- 5) Ротор 2 преобразует V в Y (таблица 1.1).
- 6) Далее сдвиг вправо на 1 ($\text{shift}_{sum3} = \text{shift}_{sum2} - \text{shift}_{R3} = 4 - 2 = 2$). $Y \rightarrow A$.
- 7) Ротор 3 преобразует A в B (таблица 1.1).
- 8) Сдвиг влево по алфавиту на 2 влево ($\text{shift}_{R3} = 2$). $B \rightarrow Z$.
- 9) Далее символ попадает на рефлектор. $Z \rightarrow T$ (таблица 1.2).

Обратная процедура:

- 10) Происходит сдвиг по алфавиту на 2 вправо ($\text{shift}_{R3} = 2$, пункт 8). Следовательно, $T \rightarrow V$.
- 11) Обратное преобразование. Символ V попадает на ротор 3 и преобразуется в L (таблица 1.1).
- 12) $\text{shift}_{sum3} = 2$ (пункт 6), поэтому необходимо сделать сдвиг в алфавите на 2 символа влево: $L \rightarrow J$.
- 13) Обратное преобразование. Символ J попадает на ротор 2 и преобразуется в B (таблица 1.1).
- 14) $\text{shift}_{sum2} = 4$ (пункт 4), перемещаемся по алфавиту на 4 буквы вправо. $B \rightarrow F$.
- 15) Обратное преобразование. Символ F попадает на ротор 1 (таблица 1.1). $F \rightarrow D$.
- 16) $\text{shift}_{sum1} = 4$ (пункт 3), поэтому необходимо сделать сдвиг в алфавите на 4 символа влево $D \rightarrow Z$.

17) Проверка на наличие символа Z на коммутационной панели.

Парного символа нет, поэтому на выход подается символ Z .

Шифрование буквы G

- 1) На вход поступает символ G , $\text{shift} = 2$.
- 2) Проверяется, нет ли у символа G парного символа в коммутационной панели. Парного символа нет, значит символ G не претерпевает изменений.
- 3) Далее происходит сдвиг на 5 вправо ($\text{shift}_{sum1} = \text{shift} + \text{shift}_{R1} = 2 + 3 = 5$). Из символа G получаем L .

И т.д.

Заключение

В преддипломной практике был рассмотрен принцип работы Машины Энигма и реализована программа с интерфейсом.

Энигма представляла собой достаточно удобную шифровальную машину: получаемый шифр был достаточно сложен, а сама процедура кодирования/раскодирования была довольно проста. Также неотъемлемым преимуществом шифра Энигмы является высокая скорость кодирования/раскодирования.

С появлением компьютеров надежность такого шифра упала, т.к. код имеет достаточно много важных особенностей, упрощающих взлом, поэтому в современных системах такое шифрование применяют достаточно редко.

Целью данной работы являлась программная реализация Машины Энигма с интерфейсом.

Были решены следующие задачи:

- Изучен принцип работы Машины Энигма.
- Разработана программа Машины Энигма с интерфейсом.
- Проведено тестирование разработанной программы.

Список использованных источников

1. Enigma wiring. [Электронный ресурс]. URL: <https://www.cryptomuseum.com/crypto/enigma/wiring.htm> (дата обращения: 23.10.2022).

2. Эмулятор шифровальной машины Enigma C# .NET. [Электронный ресурс]. URL: <https://dev.koshovyi.com/2020/12/14/emulyator-shifrovalnoj-mashiny-enigma-c-net/> (дата обращения: 23.10.2022).

3. Энигма. [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0> (дата обращения: 23.10.2022).

4. Как работает шифровальная машина Энигма. Видео. [Электронный ресурс]. URL: <https://iphonesia.ru/3169-kak-rabotaet-enigma-machina.html> (дата обращения: 23.10.2022).

5. Роль дешифровки Энигмы в победе во Второй мировой войне. [Электронный ресурс]. URL: <https://moluch.ru/young/archive/47/2524/> (дата обращения: 23.10.2022).

6. Github-репозиторий программы Машины Энигма с интерфейсом. [Электронный ресурс]. URL: <https://github.com/val-ugs/UDevMe.EnigmaApp> (дата обращения: 30.10.2022).